Department of Homeland Security
Cybersecurity and Infrastructure Security Agency
Emergency Communications Division

Communication Assets Survey and Mapping Tool

Rules of Behavior for Access Managers

(Addendum to End User ROB)

6/26/2020

DOCUMENT CHANGE HISTORY

Version	Date	Author	Description
1.0	6/26/20	J Pollard	Initial Draft

Table of Contents

1.0 INTRODUCTION

Rules of Behavior (ROB) that apply to access and use of Department of Homeland Security (DHS) information technology (IT) resources are a vital part of the DHS IT Security Program and help to ensure the security of systems and the confidentiality, integrity, and availability of sensitive information.

This Communication Assets Survey and Mapping (CASM) Access Manager (AM) ROB is an addendum to the CASM End User ROB. It informs AMs of their CASM system security responsibilities. By adhering to these rules all AMs, together, maintain CASM system and data security. The CASM AM ROB applies to each individually designated Access Manager of the CASM system. You have already read and acknowledged the CASM End User ROB, which forms the basis for this ROB.

These Rules of Behavior are consistent with the IT security policy and procedures given by DHS Management Directive 140-1, "Information Technology Systems Security", "DHS Sensitive Systems Policy Directive 4300A," and the "DHS 4300A Sensitive Systems Handbook."

Any user not in compliance with applicable Rules of Behavior is subject to sanctions that may include verbal or written warning, denial of system access for a specific period of time, reassignment to other duties, criminal or civil prosecution, or termination, depending on the severity of the violation.

The CASM system is operated and maintained by the DHS Cybersecurity and Infrastructure Security Agency's Emergency Communications Division.

2.0 REFERENCES

a) DHS Sensitive Systems Policy Directive 4300A v13, June 27, 2017
b) DHS 4300A Sensitive Systems Handbook v12.0, November 15, 2015
c) DHS Information Security Continuous Monitoring Strategy, An Enterprise View, May 14, 2014
d) DHS Directive MD Number: 140-01, Revision Number: 00, Information Technology Systems Security, 07/31/2007

3.0 AM RULES OF BEHAVIOR

The following rules of behavior apply to all Access Managers of the CASM system. Rules of Behavior apply to users at their primary workplace, while teleworking or at a satellite site, at any alternative workplaces, and while traveling.

- I understand that I may grant access to the system or any part of its data repository only to those individuals who require access for the performance of their official duties.

- I will vet individuals that request system access using supervisor information for that individual as provided in their request.
- I will close user accounts for individuals who no longer require access for official business.
- I will change access to system functions or data as the official needs of end users, whose access is under my control, change.
- If I delegate CASM AM privileges to a CASM end user, I will ensure that they acknowledge this ROB prior to delegation. The CASM Help Desk can provide the document as needed.
- I will notify the CASM Help Desk, casmhelp@cisa.dhs.gov, under any circumstances in which I can no longer meet the responsibilities outlined in this ROB.

3.1 Incident Reporting

- I will promptly report suspected IT security incidents to the CASM DHS Help Desk at casmhelp@cisa.dhs.gov. Users can report cyber security incidents and observed vulnerabilities 24/7 through the DHS website to the United States Computer Security Emergency Readiness Team (US-CERT) at https://www.us-cert.gov/report.

3.2 Accountability

- I understand that I will be held accountable for my actions while performing Access Management responsivities for the DHS CASM system.